

UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA  
Criminal No. 17-64 (DWF/KMM)

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	<b>MEMORANDUM IN</b>
	)	<b>OPPOSITION TO</b>
v.	)	<b>MOTION TO SUPPRESS</b>
	)	
EDWARD S. ADAMS,	)	
	)	
Defendant.	)	

The United States respectfully submits this Memorandum in Opposition to Edward S. Adams' ("Adams") Motion to Suppress [Docket No. 37]. The government responds as follows:

1. Adams' claim that the warrant was insufficiently particularized because it authorized Yahoo! Inc. to disclose the contents of Adams' email accounts should be denied. The search warrant incorporated the two-step process set forth in Federal Rule of Criminal Procedure 41 and approved by courts. In the first step, the warrant authorized Yahoo! to disclose the contents of email accounts to the government as specified in Section I of Attachment B to the warrant. In the second step, the government was authorized to seize emails that related to the federal criminal statutes, individuals, timeframes, and subject matter set forth in Section II of Attachment B to the warrant. The warrant was sufficiently particularized. Moreover, law enforcement's reliance upon it was objectively reasonable and the *Leon* exception accordingly applies.
2. With respect to Adams' claim that the warrant was not reasonably executed, the government will be prepared to offer evidence regarding the reasonable execution of the warrant at an evidentiary hearing.

**FACTUAL BACKGROUND**

The government in this matter executed a search warrant on two email accounts maintained by Adams through Yahoo! Inc. ([edwardsadams@yahoo.com](mailto:edwardsadams@yahoo.com) and [jafman1@yahoo.com](mailto:jafman1@yahoo.com)), as well as an account not at issue maintained by another individual.

As noted in Adams' Motion, two search warrants were issued because the first warrant was not properly served. The second search warrant, which was appropriately served, was signed by Magistrate Judge Rau in January 2016 ("email search warrant"). It is that warrant that is the focus of Adams' Motion.<sup>1</sup>

### **The Email Search Warrant**

The email search warrant Affidavit sets forth probable cause to believe that Adams and another had violated 18 U.S.C. Sections 1341 (mail fraud) and 1343 (wire fraud). Adams and another were alleged to have defrauded company shareholders and others to benefit themselves financially. Affidavit of Christie Kroells ("Affidavit") at 2-18, ¶¶ 4-34, *found at* 16-MJ-8 (SER), DCD 3 *and at* Exhibit 3 to Adams' Motion, DCD 41-1. The Affidavit also set forth probable cause to believe that evidence of the violations would be located in the two email accounts maintained by Adams through Yahoo! Inc. *See id.* at 2-3, ¶ 4; 10-11, ¶ 20; 15-16, ¶ 29; 18, ¶¶ 33-34.

The Affidavit also made plain that Adams was at material times a practicing attorney. The Affidavit stated that from at least 2008 through 2014, Adams was a partner in a Minneapolis-based law firm, Adams Monahan LLP. *Id.* at 5, ¶ 10. The law firm is referred to throughout the Affidavit with the acronym AMLLP. *See, e.g., id.* at 6-7, ¶ 12. AMLLP was material to the investigation in a number of ways, as Adams was alleged to

---

<sup>1</sup> The warrant was issued under the authority of Title 18, United States Code, Section 2703. Under § 2703, the government may compel a service provider to disclose either content or non-content information pursuant to "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." 18 U.S.C. §§ 2703(a), (b), and (c) (1) (A).

have concealed from shareholders material facts about the firm's representation of relevant entities. *See id.*

Adams' email account at his law firm was [eadams@adamsmonahan.com](mailto:eadams@adamsmonahan.com). The government did not seek a warrant for that account. Rather, the government sought emails from two personal accounts that, as specified in the Affidavit, included non-privileged communications relevant to the investigation. *See, e.g., id.* at 10-11, ¶ 20 (detailing relevant emails sent from jafman1@yahoo.com to employees of Scio); *id.* at 15, ¶ 29 (detailing relevant email sent to edwardsadams@yahoo.com account from Chief Financial Officer for Private Scio); *id.* at 18, ¶ 33 (noting that Adams provided emails to the SEC from his edwardsadams@yahoo.com account that related to his business dealings with Scio). That Adams testified to the SEC that he generally considered the edwardsadams@yahoo.com to be his primary account was included in the Affidavit. *Id.* at 18, ¶ 33.

### **Rule 41 Process**

The email warrant followed the two-step process set forth in Federal Rule of Criminal Procedure 41(e)(2)(B). Rule 41(e)(2)(B) authorizes seizure or copying of electronically stored information for later review consistent with the warrant. The pertinent Advisory Committee Notes provide that “[t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.” Fed. R. Crim. P. 41, Advisory Committee Notes to 2009 Amendments.

The email warrant set forth the two steps contemplated by Rule 41. First, the warrant authorized Yahoo! to disclose to the government electronically stored information associated with edwardsadams@yahoo.com and jafman1@yahoo.com, as well as a third account not at issue here. *See* Email Search Warrant, Attachment A & Attachment B, Section I, *found at* 16-MJ-8 (SER), DCD 3 *and at* Exhibit 3 to Adams' Motion, DCD 41-1 at 69-70. The warrant authorized the disclosure of the equivalent of the entire storage medium, that is, *inter alia*, the content of all emails associated with the account. *See* Attachment B at Section I(a).

In step two, Judge Rau authorized the government to seize information particularized as follows in Section II:

## **II. Information to be seized by the government**

- a. All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 United States Code, Sections 1341 and 1343, those violations involving Edward S. Adams and Michael R. Monahan and occurring after October 25, 2006, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:
  1. All documents, records, and communications related to financial, bookkeeping, transactional, and tax records reporting the business and financial transactions of ADI, ADGC, Private Scio, Public Scio, Focus, and ESA during and for the calendar, fiscal, and federal tax years 2010 to present; to include, but not limited to:
    - i. All bookkeeping ledgers, journals, reports, and other bookkeeping records, and computer printouts thereof, which itemize and record the dates, amounts, purpose, and expense category and classification of all financial transactions conducted in and through the business bank

accounts and other financial accounts of the above business entities.

- ii. All bookkeeping ledgers, journals, reports, and other bookkeeping records, and computer printouts thereof, which record, identify, and itemize the dates, amounts, and nature and classification of all income and expenses of the above business entities.
2. All documents, records, and communications related to Private Scio, Public Scio, to include all such documents, records, and communications regarding the AD II ADGC proxy statement from March 2011, the asset purchase agreement between P.J)/AGC and Private Scio, the stock-repurchase program, and the private offering.
3. All documents and records reflecting communications with shareholders or prospective shareholders of ADI, ADGC, Private Scio, and Public Scio.

Attachment B, Section II (“Section II”). Consistent with Rule 41, the government undertook step two review of the content after it was disclosed by Yahoo!

### **ARGUMENT**

#### **I. THE EMAIL SEARCH WARRANT WAS SUFFICIENTLY PARTICULARIZED.**

To effectuate the search and seizure, Judge Rau approved and the government employed the two-step process for electronic evidence set forth in Federal Rule of Criminal Procedure 41(e)(2)(B). Courts have concluded that the Rule 41’s two-step process comports with constitutional standards. That process contemplates as its first step the production of the entire contents of the electronic storage medium, in this instance the contents of the email accounts stored on Yahoo!’s servers.

Adams nonetheless claims that Judge Rau sanctioned an insufficiently particularized warrant by authorizing Yahoo! to produce the contents of Adams' email accounts. Adams Br. at 20-26. Adams' claim should be rejected. The email warrant comported with Rule 41 and constitutional particularity standards.

## **A. Legal Standards**

### **1. Warrant Clause**

The Warrant Clause of the Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” A search warrant complies with the Fourth Amendment when it includes three elements: it must be issued by a neutral magistrate; it must be based on a showing of “probable cause to believe that ‘the evidence sought will aid in a particular apprehension or conviction’ for a particular offense”; and it must satisfy the particularity requirement. *Dalia v. United States*, 441 U.S. 238, 255 (1979).

### **2. Particularity**

“To satisfy the particularity requirement of the Fourth Amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized.” *United States v. Sigillito*, 759 F.3d 913, 923 (8th Cir. 2014) (citation omitted). “The degree of specificity required will depend on the circumstances of the case and on the type of items involved.” *United States v. Summage*, 481 F.3d 1075, 1079 (8th Cir.2007). Thus, “[t]his particularity standard is one of practical accuracy rather

than of hypertechnicality.” *Sigillito*, 759 F.3d at 923 (quotation marks and citation omitted).

### **3. Rule 41’s Two-Step Procedure for Electronic Evidence**

Rule 41(e)(2)(B) specifies that a warrant “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.” The Advisory Committee Notes explain that the two-step process is “inherent in searches for electronically stored information.” Fed. R. Crim. P. 41, Advisory Committee’s Notes to 2009 Amendments. The Notes recognize that electronic storage media “commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location.” *Id.* The Rule accordingly “acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.” *Id.*

#### **B. The Email Warrant Was Sufficiently Particularized.**

The Adams email warrant follows Rule 41’s two-step approach for the seizure of electronic evidence. The warrant in step one sets forth with particularity the location to be searched, namely information associated with Adams’ two email accounts stored at the premises of Yahoo! Inc. *See* Attachment A. The information included the content of all emails associated with the accounts. *See* Attachment B, Section II(B)(1)(a). In authorizing the disclosure of the entire account, Judge Rau approved the warrant in keeping with Rule

41's acknowledgment that "officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41, Advisory Committee's Notes to 2009 Amendments.

In step two, the warrant particularized the information the government was authorized to seize. The government was authorized to seize information from the specified email accounts that "constitutes fruits, contraband, evidence and instrumentalities of violations of 18 United States Code Sections 1341 and 1343." *See* Attachment B, Section II(a). The warrant further specified that those violations were "involving Edward S. Adams and Michael R. Monahan" and "occurring after October 25, 2006." *Id.* Information to be seized included (1) documents, records, and communications related to financial transactions of the subject companies from 2010 to present; (2) documents, records, and communications related to the Scio entities; and (3) documents and records reflecting communications with prospective shareholders of the subject companies. *See* Attachment B, Section II(a) (1)-(3).

Taken together, the warrant specified the email accounts to be searched, the criminal violations being investigated, individuals believed to be associated with those violations, and relevant subject matter. Far from a general warrant, the Adams email warrant was "sufficiently definite to enable the searching officers to identify the property authorized to be seized." *Sigillito*, 759 F.3d at 923.

Judge Rau did not authorize novel or unprecedented warrant procedures here, but rather issued a warrant that followed Rule 41 process promulgated by the Supreme Court. *See* 28 U.S.C. § 2072. Reviewing courts have approved of Rule 41's two-step process for

email warrants, including the step-one disclosure of the entire contents of email accounts as provided for in the Rule. Even before Rule 41 was amended to explicitly incorporate the two-step process, the Eighth Circuit upheld as reasonable the execution of a two-step warrant under 18 U.S.C. § 2703 for email stored with a web-based email provider. *See United States v. Bach*, 310 F.3d 1063, 1067-68 (8th Cir. 2002). Bach, an investigator “obtained a state search warrant to retrieve from Yahoo! e-mails between the defendant and possible victims of criminal sexual conduct, as well as the Internet Protocol addresses connected to his account.” *Id.* at 1065. However, Yahoo! employees did not attempt to find this particular information:

Yahoo! technicians retrieved all of the information from Bach's account at dlbg15@yahoo.com and AM's Yahoo! e-mail account. According to Yahoo!, when executing warrants, technicians do not selectively choose or review the contents of the named account. The information retrieved from Bach and AM's accounts was either loaded onto a zip disc or printed and sent to [a law enforcement officer]. E-mails recovered from Bach's account detail him exchanging pictures with other boys and meeting with them.

*Id.* The court upheld the search as reasonable under the Fourth Amendment. *Id.* at 1067-68.

Adams attempts to distinguish *Bach* on the ground that the email account at issue there turned out to contain six emails. Adams Br. at 24-25, n.5. The number of emails disclosed upon execution of the warrant does not inform whether disclosure of all email account content was appropriately authorized in the first instance. The warrant in *Bach* used the same two-step process employed in this matter, and the number of emails disclosed was not determinative in concluding the search was constitutional.

Other courts have concluded that disclosure of the entire contents of an email account as contemplated by Rule 41 passes constitutional muster. For example, in *United States v. Patel*, the defendant asserted that an email warrant authorizing the disclosure of the entire contents of an email account was insufficiently particularized. *United States v. Patel*, 2017 WL 3394607 at \*3 - \*4 (S.D.N.Y. August 8, 2017) (unpublished). The court noted that because the enormity of data on computers and in email accounts rendered on-site searches impractical, “when armed with a search warrant describing with particularity the types of emails to be searched, the Government may obtain the contents of an email account and then conduct a review to determine which emails fall within the warrant’s scope.” *Id.* at \*3 (citations omitted). The review conducted to determine which emails fall within the warrant’s scope must be limited to the search for and seizure of evidence of specified crimes, not a general rummaging for evidence of any crime. *Id.* Under these “long recognized” principles, “[a] warrant therefore does not violate the Fourth Amendment’s particularity requirement where it permits the Government to obtain the entire contents of the email account to determine which particular emails come within the search warrant.” *Id.* at \*4 (quotation marks and citation omitted). Other courts are in accord. *In the Matter of the Search of Information Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation*, 212 F.Supp.3d 1023, 1037 (D. Kan. 2016) (“And while Rule 41(e) (2) leaves open the question of particularity when the government seeks ESI, the majority of case law relating to the search of an email account has upheld the Government’s ability to obtain the entirety of the account to then search for relevant evidence.”); *United States v. Skully*, 108 F.Supp.3d 59, 92-95 (E.D.N.Y. 2015)

(discussing issues and authority at length in rejecting defendant’s claim that Yahoo! email search warrants were “overly broad and insufficiently particularized in violation of the Fourth Amendment because they mandated disclosure of the entire contents of email accounts and seizure of those emails”); *United States v. Tsarnaev*, 53 F. Supp. 3d 450, 463-64 (D. Mass. 2014) (concluding that email search warrant and search procedure that complied with Rule 41’s two-step process satisfied particularity standards); *United States v. Taylor*, 764 F. Supp.2d 230, 237 (D. Me. 2011).

Adams asserts that “[w]ithout a warrant that specifies limitations to at least time period, specific senders and recipients associated with the conduct under investigation, or other criteria designating the particular facts being investigated, the search of a citizen’s entire email is unconstitutional.” Adams Br. at 24-25. The warrant does, however, specify limitations designating the particular facts being investigated, including reference to the relevant criminal statutes and subject matter, while also identifying individuals under investigation by name. The search of the email accounts specified in the warrant was sufficiently particularized.

To the extent Adams suggests that Yahoo! should have been directed to apply his suggested “criteria designating particular facts being investigated” to email content before providing emails to the government, the suggestion should be rejected. As is discussed above, neither Rule 41 nor particularity principles require Yahoo! to cull email content in step one of the Rule 41 process. Nor is converting email service providers into government search agents a required – or even preferable – approach. *See, e.g., In the Matter of the Search of Information Associated with [redacted]@mac.com*, 13 F.Supp.3d 157, 165-66

(D.D.C. 2014) (reviewing why “[e]nlisting a service provider to execute the search warrant could also present nettlesome problems”); *United States v. Deppish*, 994 F.Supp.2d 1211, 1220 (D. Kan. 2014) (“[N]othing in the Fourth Amendment requires law enforcement to cede to non-law enforcement their power to search and determine which matters are subject to seizure”); *Taylor*, 764 F. Supp. 2d at 237 (“The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.”); *Bowen*, 689 F. Supp. 2d at 682.<sup>2</sup>

The authority relied upon by Adams does not require suppression. Adams, for example, heavily relies upon *United States v. Cioffi*. Adams Br. at 21. In *Cioffi*, the district court reviewed a search warrant that required Google to turn over the contents of the defendant’s personal email account. *United States v. Cioffi*, 668 F.Supp.2d 385, 388-89 (E.D.N.Y. 2009). The warrant, however, did not include a second step further limiting law enforcement seizure of email in the account to specific categories of evidence or in relationship to specified crimes; instead, it broadly authorized seizure of “all e-mail up through August 12, 2007.” *Id.* Although the warrant incorporated and attached an attachment, the attachment also authorized the government to seize defendant’s emails with

---

<sup>2</sup> For example, Adam’s argument that an email warrant should direct a service provider like Yahoo! to disclose email to or from or to specified recipients or senders is neither required nor practicable. Law enforcement generally cannot know, and did not know in this case, in advance of obtaining a search warrant everyone with whom one under investigation is communicating regarding his alleged criminal activity or all of the email accounts/addresses individuals may be using.

“no provision limiting the emails to be seized to those containing evidence of the crimes charged in the indictment or, indeed, of any crime at all.” *Id.* at 389. The crimes under investigation were identified in the search warrant affidavit, but because the affidavit had not been attached and incorporated in the warrant itself, the *Cioffi* court did not consider it. *Cioffi*, 668 F.Supp.2d at 388. Under those circumstances, the court concluded that whatever the particularity required for computer searches, the warrant was overbroad because it authorized a search for “evidence of *a* crime, that is to say any crime.” *Id.* at 392. *Cioffi*, then, is illustrative of the particularity defect discussed in *Patel* and not present in this case, where the review of the content of the entire email account was not limited to evidence of specified crimes, but rather authorized general rummaging for evidence of any crime.

Unlike in *Cioffi*, the warrant here attached and incorporated an attachment that identified with particularity the crimes about which evidence was being sought. Attachment B to the warrant authorized the government to seize information that “constitutes fruits, contraband, evidence and instrumentalities of violations of [Title] 18 United States Code, Sections 1341 and 1343.” *See* Attachment B at Section II(a). The particularity absent in *Cioffi* was present here.

Adams also relies heavily on the *Target Email Accounts* case. Adams Br. at 22. The magistrate judge in that case sought to impose a number of *ex ante* restrictions on an email warrant, including having the email provider cull content from the subject email accounts before disclosure. The Kansas district court, however, subsequently rejected the magistrate’s reasoning as “clearly erroneous or contrary to law,” and approved email

warrants that authorize disclosure of the entire contents of the email accounts. *See In the Matter of the Search of Information Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation*, 212 F.Supp.3d 1023, 1037 (D. Kan. 2016); *see also United States v. Deppish*, 994 F.Supp.2d 1211, 1221 (D. Kan. 2014) (disagreeing with *Target Email Accounts* and distinguishing it based upon the magistrate judge's reliance on cases where warrant failed to refer to any particular criminal statute whatsoever to limit seizure of items). The district court relied upon Rule 41's two-step process and the case law construing it to conclude that an email warrant is sufficiently particularized if it authorizes in step one disclosure of all contents from particularized email accounts and identifies with particularity in step two what evidence the government intends to seize. *In the Matter of the Search of Information Associated with Email Addresses Stored at Premises Controlled by the Microsoft Corporation*, 212 F.Supp.3d at 1037.

Other courts have similarly distinguished *Cioffi* and rejected the reasoning underlying the *Target Email Accounts* case and its brethren. *See, e.g., Skully*, 108 F.Supp.3d at 92-95. The remaining district court authority cited by Adams (*United States v. Shah*, *In re [REDACTED]@gmail.com*, and *In re Search of Google Email Accounts Identified in Attachment A*, cited at Adams Br. at 22-23) are distinguishable on the same grounds. In addition, the warrant at issue in *Shaw* was much less particularized with respect to the items to be seized than the warrant at issue here. *See United States v. Shah*, 2015 WL 72118 at \*13-\*14 (E.D.N.C. 2015) (unpublished) (reviewing warrant that lacked any particularity of items to be seized beyond a generic statutory reference to a computer fraud crime). *Shah* also supports the government's positions herein as to applicability of the

*Leon* good faith exception (*Shah* at \*15-16), the use of Rule 41’s two-step process (*Shah* at \*16-\*17), the absence of particular search methods within the warrant itself (*Shah* at \*18-\*19), and the questioning of the reasoning of the *Target Email Accounts* case even in its own jurisdiction (*Shah* at \*18).

Adams further relies upon a concurrence in the Ninth Circuit’s *United States v. Comprehensive Drug Testing, Inc.* decision. Adams Br. at 23-24. As the Third Circuit very recently noted, the *ex ante* protocols identified in that concurrence, which is not binding even in the Ninth Circuit, have not been adopted by subsequent Ninth Circuit panels. *United States v. Perez*, 2017 WL 4679583 at \*2 (3d Cir. Oct. 18, 2017) (unpublished) (“Notably, the Ninth Circuit reissued the [*Comprehensive Drug Testing*] opinion about a year later as a per curium opinion, which differed little except that it moved the guidance protocols to a (non-binding) concurrence. As a result, subsequent Ninth Circuit panels have upheld broad warrants authorizing searches of all a target’s digital storage devices and media despite the absence of precautionary search protocols.” (quotation marks and citations omitted)).

Adams relatedly reiterates two cases, *Target Email Accounts* and *Comprehensive Drug Testing*, in connection with his claim that *ex ante* filtering procedures “are required.” Adams Br. at 28. As is discussed above, the reasoning of the *Target Email Accounts* case was repudiated as clearly erroneous or contrary to law by the reviewing court in Kansas, and the protocols referenced in *Comprehensive Drug Testing* are not required even in the Ninth Circuit. See generally *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (“Nothing in the language of the Constitution or in this Court’s decisions interpreting that language

suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.” *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (quoting *Dalia v. United States*, 441 U.S. 238, 255 (1979) (ellipses added)). Rather, “the details of how best to proceed with the performance of a search authorized by warrant” are “generally left to the discretion of the executing officers.” *Dalia*, 441 U.S. at 257.

Adams also cites to *United States v. Blake* with respect to particularity. *See* Adams Br. at 22. The Eleventh Circuit decided *Blake* on *Leon* good-faith rather than particularity grounds. *See United States v. Blake*, 868 F.3d 960, 974-75 (11th Cir. 2017). Whether the court would have concluded that the Facebook social media warrants at issue were sufficiently particularized is uncertain at best. While the *ex ante* limitations discussed by the court in dicta were viewed as preferable because they would “undermine any claim” that the Facebook warrants were general warrants, the court did not opine on whether the warrants were nonetheless sufficiently particularized. *See generally Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995) (noting that the Supreme Court had “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment”).<sup>3</sup>

---

<sup>3</sup> One district court in the Eleventh Circuit has cited *Blake* in connection with the issuance of email search warrants. *See United States v. In the Matter of the Search of Information Associated with Fifteen Email Addresses*, 2017 WL 4322826 at \*5-\*7 (M.D. Alabama Sept. 28, 2017). The magistrate in that case requested that the government add temporal restrictions to the emails to be disclosed, the government agreed, and the district court approved the temporally-limited warrants. As is noted herein, *Blake* did not decide whether such limitations were constitutionally required in connection with the Facebook warrants that it reviewed or otherwise, and courts have appropriately concluded that disclosure of the entire content of email accounts with subsequent seizure of particularized information is constitutional.

The two-step process employed by the government here was consistent with Rule 41 and relevant authority. The government appropriately requested the content of email accounts in step one with authority to seize emails in step two as set forth in Attachment B. Adams' motion to suppress on particularity grounds should accordingly be denied.<sup>4</sup>

## **II. THE WARRANT WAS SECURED IN GOOD FAITH.**

### **A. Legal Standard**

In *United States v. Leon*, 468 U.S. 897, 926 (1984), the Supreme Court rejected suppression of evidence obtained by officers acting in objectively reasonable reliance on a search warrant: "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." Consistent with *Leon*, the Eighth Circuit has identified four circumstances where the *Leon* good faith exception does not apply:

(1) the supporting affidavit or testimony includes a false statement made knowingly and intentionally or with reckless disregard for the truth to mislead the issuing judge; (2) the issuing judge 'wholly abandoned his judicial role' in issuing the warrant; (3) the affidavit in support of the warrant is 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'; or (4) the warrant is 'so facially deficient' that no police officer could reasonably presume the warrant to be valid.

---

<sup>4</sup> Adams includes within his particularity section a discussion of the manner in which the warrant was executed, namely with respect to attorney-client communications. Adams Br. at 26-29. The government will be prepared to present evidence on the reasonableness of the execution of the warrant at a motions evidentiary hearing.

*United States v. Proell*, 485 F.3d 427, 430 (8th Cir. 2007) (emphasis omitted) (quoting *Leon*, 468 U.S. at 923); *see also United States v. Ortiz-Cervantes*, 868 F.3d 695, 702–03 (8th Cir. 2017) (same).

Adams suggests that suppression is appropriate under *Leon* regardless of whether the alleged misrepresentation or omission is material to the warrant’s issuance. Adams Br. at 32. The Eighth Circuit has recognized that materiality attends *Leon*. *See, e.g., United States v. Pruett*, 501 F.3d 976, 982 (8th Cir. 2007) (reviewing claim that *Leon* did not apply because affiant included “false facts and omitted material facts” and denying it in part because even if contested information had been included in the affidavit, the Court “did not believe it would have changed the magistrate’s probable cause analysis”); *United States v. Lakoskey*, 462 F.3d 965, 975, 977-78 (8th Cir. 2006) (rejecting blended *Franks/Leon* claim in part because inclusion of allegedly material information that was not in warrant application would not have altered probable cause determination); *United States v. Humphrey*, 140 F.3d 762, 765 (8th Cir. 1998) (rejecting claim that *Leon* did not apply in part because defendant “had not pointed out any material misstatements or omissions in the supporting affidavit”); *United States v. Skorniak*, 59 F.3d 750, 754-55 (8th Cir. 1995) (same); *United States v. Tagbering*, 985 F.2d 946, 951 (8th Cir. 1993) (same); *United States v. Sager*, 743 F.2d 1261, 1265-66 (rejecting claim that *Leon* exception did not apply in part because defendant had not shown affiant had falsely or in reckless disregard misstated any material fact). The District of Minnesota case cited by Adams is not to the contrary, as it notes that with respect to *Leon*-derived claims a magistrate was misled by false information intentionally or recklessly included in an affidavit, “[p]resumably, issuing magistrates

would be misled only by relevant considerations.” *United States v. Boyce*, 601 F.Supp. 947, 955 (D. Minn. 1985); *see generally, e.g., United States v. Adams*, 2014 WL 12687830 at \*6 (D. Minn. 2014) (RHK/LIB) (R&R of Judge Brisbois noting in construing *Leon* that defendant had not claimed affidavit contained “false information or material omissions”), *adopted in* 2014 WL 126968782.<sup>5</sup>

## **B. The Good Faith Exception Applies.**

Law enforcement was entitled to rely upon Judge Rau’s warrant, and the *Leon* good faith exception applies. Judge Rau did not abandon his detached and neutral role, the affidavit did not contain false statements or reckless disregard for the truth to mislead Judge Rau, the affidavit contained ample indicia of probable cause, and the warrant was not deficient, much less so facially deficient that no reasonable officer could presume it to be valid. Under these circumstances, the *Leon* good faith exception applies and suppression is not an appropriate remedy even had the warrant been insufficiently particularized. *See, e.g. Blake*, 868 F.3d at 974 (holding that *Leon* good faith exception applies even if warrant not sufficiently particularized); *Shah*, 2015 WL at \*15-\*16 (concluding that *Leon* good

---

<sup>5</sup> The Northern District of Ohio case cited by Adams reviewed the deliberately inaccurate information presented in the affidavit through the lens of finding that the probable cause set forth in the affidavit was insufficient and “fraudulently and deliberately incomplete.” *United States v. Alexander*, 740 F.Supp. 437, 448 (N.D. Ohio 1990). As argued herein, the omissions alleged by Adams would not and did not undermine the probable cause determination made by Judge Rau.

faith exception applies even where warrant not sufficiently particularized in part because law enforcement entitled to rely on courts' approval of Rule 41's two-step process).<sup>6</sup>

Adams does not claim that Judge Rau was not neutral and detached or that the affidavit lacked sufficient indicia of probable cause. Adams does claim that Judge Rau was misled by information in the affidavit that Adams asserts the affiant knew or should have known was false. Adams Br. at 31-33. Adams' claim is without merit. There is no false information in the affidavit. With respect to alleged omissions, Adams falsely asserts that Inspector Kroells did not inform Judge Rau that Adam claimed one of the email addresses was his primary email address. *Cf.* Affidavit at 18, ¶ 33 *with* Adams Br. at 32 ("The inspector did not inform Magistrate Judge Rau that . . . one of the email addresses at issue was his primary email address.").

Nor are the omissions relied upon by Adams – namely that Adams had retained counsel in SEC and civil proceedings, that Adams had a general counsel title at Apollo Diamond, and that Judge Mayeron's issuance of the warrant including a search addendum – material to probable cause or misleading. *See* Adams Br. at 32. That Adams was represented in connection with the SEC investigation and shareholder suits was not

---

<sup>6</sup> To the extent Adams is contending that execution of the warrant on his email accounts resulted in seizure of some emails outside the scope of items to be seized, the appropriate remedy is suppression of the items outside the scope, not suppression of all evidence. *See, e.g., United States v. Tenerilli*, 614 F.3d 764, 771 (8th Cir. 2010); *see generally United States v. Dahl*, 2013 WL 6175711 at \*10 (D. Minn. 2013) (PAM/JSM) (unpublished) (discussing Eighth Circuit's decision in *Dahl* and noting that items seized within scope of a warrant executed in the proper place are not suppressed even if there are items seized outside the scope that are suppressed).

relevant to probable cause underlying the allegations contained in the warrant Regarding the general counsel title at Apollo,<sup>7</sup> the government did not attempt to secure any information from Apollo or any email account of Adams at Apollo. Nor was Adams' General Counsel title relevant to probable cause underlying the allegations contained in the warrant.<sup>8</sup>

As to the search warrant addendum, as the Court is aware, the addendum used by Judge Mayeron or a similar addendum is sometimes included, either by the court or the government, in search warrants for electronically stored information. The search warrant addendum attached to the warrant signed by Judge Mayeron is a modified version of the standard search warrant addendum the government typically attaches to warrants for seizure of electronic storage devices, e.g. computers or cell phones, not to warrants for email account content. The government does not typically include the standard (or a modified) addendum in connection with email warrants, and neither do all judges. Reference to or inclusion of an addendum is not required, not referencing it was not

---

<sup>7</sup> Adams' role as General Counsel at Apollo morphed with his executive roles. *See* Adams SEC Testimony, Aug. 27, 2015, at 87 (Adams testifying that "the general counsel role [at Apollo] really kind of morphed into more of an executive role at the company versus a legal role.").

<sup>8</sup> Adams' representation of Apollo Diamond through AMLLP was relevant to the fraud allegations summarized in the Affidavit, and the fact of that representation was reflected in the Affidavit. The government stated that Adams was a practicing attorney; was a partner at his law firm AMLLP; and that Adams and AMLLP represented Apollo Diamond (referred to as ADI and ADGC in the Affidavit) on material matters. *See, e.g.*, Affidavit at 7, ¶ 12 (noting fraudulent nondisclosure that Adams and AMLLP acted as counsel for Apollo Diamond in connection with a relevant transaction).

material or misleading, and that Judge Rau issued the warrant without appending the addendum was within Judge Rau's discretion and does not undermine application of *Leon*. See, e.g., *Tsarnaev*, 53 F.Supp.3d at 462-63 (concluding that filter procedure not required in the warrant and application of *Leon* exception not undermined by its absence).

Adams' next contention is largely reiterative of his first claim. Adams contends that reliance on Judge Rau's warrant was not objectively reasonable because his general counsel title, representation by counsel in the SEC and civil matters, and the manner of the warrant's execution were not in the Affidavit. Adams Br. at 33-34. For the reasons stated herein, inclusion of those items was not material to the warrant's issuance, and law enforcement's reliance on the warrant was objectively reasonable.

Adams also incorporates by reference within his *Leon* claim his argument that the manner in which the warrant was executed was not reasonable and makes assertions about the impact of that claim on a *Leon* analysis. Adams Br. at 34. Adams' clipped quotation from *Leon* and the authority he cites do not support the notion that suppression is the appropriate remedy for his reasonableness claim or that *Leon* is inapplicable. The mostly state court cases Adams cites applying *Leon* to a warrant with respect to "execution" are concerned with searching a vehicle or place that was not the subject of the warrant at all (*Parks* and *Sadie*) and the necessity for no-knock entry (*Moland* and *Cohen*). Those applications are consistent with the footnote in *Leon* providing when read in full context that "the deterrent effect of excluding evidence obtained in reasonable reliance on a subsequently invalidated warrant assumes, of course, that the officers properly executed the warrant and searched only those places and for those objects that it was reasonable to

believe were covered by the warrant.” *Leon*, 468 U.S. at 918 n.19. These circumstances are not analogous to the search of email accounts, indisputably the subject of a warrant, for items authorized to be seized. In that context, for example, the remedy for alleged seizure of items outside the scope of the warrant may be suppression of those items, not suppression of all email evidence. *See supra* note 7.

Insofar as Adams’ claims are predicated in part on what appear to be assertions that the prosecution team accessed actually privileged documents and/or is tainted by that alleged access, those claims are premature. The filter team cannot evaluate and litigate, if necessary, Adams’ claims of privilege given that Adams has not engaged the filter team in a review process. Adams Br. at 16 n.3. That process will require consideration of a number of issues. For example, counsel for Scio, the successor company to Apollo Diamond and Apollo Diamond Gemstone Corporation, waived in June 2016 any assertion of attorney-client privilege that it may hold for work performed by Adams, Monahan, or their law firm, Adams Monahan LLC, in connection with the Apollo Diamond entities or in connection with the transactions by which the assets of Apollo Diamond entities were transitioned to or acquired by Scio entities. Not until privilege matters are agreed upon or litigated is an assessment of any alleged prosecution team exposure to actually privileged materials even possible. *See, e.g., Taylor*, 764 F.Supp.2d at 238 (“Identifying such e-mails as ‘arguably privileged’ would be simply an intermediate step in determining whether they are actually privileged. Otherwise, they are not subject to protection.”)

**CONCLUSION**

Adams' motion to suppress on warrant particularity grounds should be denied for the reasons set forth herein. The government will be prepared to present evidence at a motions evidentiary hearing on Adams' claim that the warrant was not reasonably executed.

Dated: November 15, 2017

Respectfully Submitted,

GREGORY S. BROOKER  
Acting United States Attorney

s/David M. Genrich

BY: DAVID M. GENRICH  
DAVID M. MARIA  
JOHN E. KOKKINEN  
Assistant United States Attorneys